POLICE OMBUDSMAN FOR NORTHERN IRELAND

Data Protection Appropriate Policy Document for Law Enforcement Processing

(Part 3 and schedules 7 and 8 of the Data Protection Act 2018)

POLICY OWNER:	Chief Executive Officer
POLICY APPROVED BY:	Senior Management Team
IMPLEMENTATION DATE:	26/02/2020
VERSION:	1.1
NEXT REVIEW:	August 2024

Contents

Data Protection Policy Document
for processing for Law Enforcement Purposes
(Part 3 and Schedules 7 and 8 of the Data Protection Act 2018)

1 Scope

1.1 This Data Protection Policy Document applies to the processing of personal data for law enforcement purposes and also to sensitive processing for those purposes where it is necessary for the purposes of the Ombudsman and her staff to carry out the functions of the Office of the Police Ombudsman for Northern Ireland (the Office).

1.2 This policy should be read in conjunction with the Office's Data Protection Policy Statement and Privacy Notices. Processing personal data for law enforcement purposes is lawfully provided such processing is carried out in accordance with the Police (Northern Ireland) Act 1998 (the 1998 Act), (together with related legislation and regulations); and the Data Protection Act 2018 (DPA 2018).

1.3 The Office may also process personal data in order to comply with statutory and legal obligations including, but not limited to:

- responding to data subject requests under the Data Protection Act 2018
- responding to requests for information under the Freedom of Information Act 2000
- obligations under section 75 of the Northern Ireland Act 1998 to ensure equality of opportunity
- maintaining records for the purposes of the Regulation of Investigatory Powers Act 2000 and Investigatory Powers Act 2016 (and related Codes of Practice).

1.4 Where appropriate the Office may use pseudonymization and anonymization measures in order to protect a person's identity where data is used for research and statistical analysis and in our public statements made pursuant to section 62 of the 1998 Act. This policy does not apply to information relating to deceased persons as the DPA 2018 applies only to data relating to living individuals who are identifiable.

1.5 This policy has been approved by the Senior Management Team (SMT). The Police Ombudsman and her staff must comply with this policy and all related data protection policies and procedures.

2 Definitions

2.1 "Processing" is defined as:

"an operation or set of operations which is performed on information, or on sets of information such as –
(a) collection, recording, organisation, structuring or storage,
(b) adaptation or alteration,

(c) retrieval, consultation or use,
(d) disclosure by transmission, dissemination or otherwise making available,
(e) alignment or combination, or
(f) restriction, erasure or destruction"

2.2 "Data subject" means the identified or identifiable living individual to whom personal data relates.

2.3 "Personal data" means any information relating to an identified or identifiable living individual (subject to subsection (14)(c).

2.4 "Sensitive processing" under section 35 of the DPA 2018 is defined as -

(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

(b) the processing of genetic data, or of biometric data, for the purposes of uniquely identifying and individual;

(c) the processing of data concerning health;

(d) the processing of data concerning an individual's sex life or sexual orientation.

2.5 "Law enforcement purposes" are the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

2.6 A "competent authority" under Schedule 7 of the DPA 2018 is defined as "any United Kingdom government department other than a non-ministerial government department". The Police Ombudsman for Northern Ireland is listed as a competent authority at paragraph 20 of Schedule 7.

2.7 A "Controller" under section 32 of the DPA 2018 means the competent authority which, alone or jointly with others -

(a) determines the purposes and means of the processing of personal data, or

(b) is the controller by virtue of subsection (2).

2.8 "Section 63 of the 1998 Act" provides for a statutory prohibition on the Ombudsman and her staff in relation to the disclosure of information subject to a number of specific exceptions (see Appendix A for full text of section 63).

3 Purpose of the Appropriate Policy

3.1 Processing of personal data for law enforcement purposes must comply with the data protection principles outlined in Part 3 of the DPA 2018. Specifically, the first data protection principle (section 35) states that processing for law enforcement purposes must be lawful and fair. Where the processing by the Ombudsman and her staff is sensitive processing for any law enforcement purpose, an appropriate policy must be in place and that processing is permissible in two cases.

(i) the data subject has given consent to the processing for that purpose

or

(ii) is *strictly necessary* for the law enforcement purpose and is based on one of the conditions outlined in schedule 8 of the DPA 2018 as required by section 35(5) of the DPA 2018.

3.2 This document is the Appropriate Policy document as required by section 35(4) of the DPA 2018.

4 Introduction

4.1 The Office of the Police Ombudsman for Northern Ireland was established under Part VII of the 1998 Act. The Police Ombudsman must exercise her powers so as to secure an efficient, effective and independent police complaints system, and to do so in the way she thinks best calculated to secure the confidence of the public and of the police in that system (section 51(4) of the 1998 Act).

4.2 The Police Ombudsman has jurisdiction in respect of complaints about the following organisations when operating in Northern Ireland:-

- The Police Service of Northern Ireland including designated civilians
- The Belfast Harbour Police
- The Belfast International Airport Police
- The Ministry of Defence Police
- The National Crime Agency

4.3 In addition, the Police Ombudsman has jurisdiction to investigate serious[1] complaints about:

- Mutual Aid police officers from Great Britain
- Certain Home Office employees (Immigration officers, designated customs officials and custom revenue officials)

4.4 The processing of personal data by the Police Ombudsman includes processing for the purpose of the detection of crime, apprehension and prosecution of offenders, maintenance of law and order and provision of a regulatory system which protects members of the public against dishonesty, malpractice or other improper conduct or unfitness by police officers.

5 The Police (Northern Ireland) Act 1998

5.1 Part VII of the 1998 Act provides for the independent investigation of complaints about the police.

[1] Serious complaints are defined at Schedule 1 of the agreements made pursuant to sections 60, 60ZA, 60ZB AND 60ZC of the 1998 Act.

- Section 51 of the 1998 Act provides that there shall be a Police Ombudsman for Northern Ireland who shall exercise her power in such manner and to such extent as appears to her to be best calculated to secure:
  (a) the efficiency, effectiveness and independence of the police complaints system; and
  (b) the confidence of the public and of members of the police force in that system.
- Section 52 provides for the receipt and initial classification of complaints.
- Section 53 provides for the informal resolution of the complaints.
- Section 54 provides for the formal investigation of complaints.
- Section 55 provides for the Policing Board, Department of Justice, Secretary of State and Chief Constable to refer certain matters to the Ombudsman for her consideration.
- Section 55 (6) enables the Ombudsman of her own motion/initiative to formally investigate matters where it appears to her that it is desirable in the public interest that she should do so.
- Section 56 outlines how the Ombudsman shall conduct a formal investigation.
- Section 58 outlines steps to be taken after the investigation should the Ombudsman determine that criminal proceedings are appropriate.
- Section 59 outlines steps to be taken after the investigation should the Ombudsman determine that disciplinary proceedings are appropriate.
- Section 60 enables the Ombudsman to enter into an agreement with an authority maintaining a body of Constables where such constabularies are not maintained by the Policing Board, subject to the approval of the Department of Justice.
- Section 61 requires the Ombudsman to provide reports to the appropriate authorities on matters relating generally to the functions of the Ombudsman.
- Section 61AA allows the Ombudsman to provide such statistical information and any other general information as is required to enable the Policing Board to carry out its functions.
- Section 62 allows the Ombudsman to publish a statement as to her actions, her decisions and determinations and the reasons for these.
- Section 63 places restrictions on the disclosure of information obtained by the Ombudsman and her staff.

5.2 For further information on the functions of the Office, please visit the website at www.policeombudsman.org

6 Conditions for processing of personal data and sensitive processing for law enforcement purposes

6.1 The Police Ombudsman is required to process personal data for law enforcement purposes in accordance with the data protection principles

provided for in sections 35 to 40 of the DPA 2018. In addition sections 35,36,38 and 39 makes provision to supplement each of those principles to which it relates and sections 41 and 42 of the DPA 2018 makes provision about the safeguards for archiving and for sensitive processing.

6.2 As a controller, the Police Ombudsman must meet the additional safeguards for archiving and sensitive processing. In particular in relation to sensitive processing the Schedule 8 conditions listed below apply to sensitive processing.

6.3 Sensitive processing is only permitted in two cases. The first is where the data subject has given consent to the processing and at the time when the processing is carried out the controller has an appropriate policy in place in accordance with section 42 of the DPA 2018. The steps taken by the Office to obtain consent for the purposes of law enforcement are outlined at paragraph 6.4 below. The second case is where the processing is strictly necessary for law enforcement purposes and at least one Schedule 8 condition is met and an appropriate policy is in place in accordance with section 42. The following Schedule 8 conditions apply to sensitive processing for law enforcement purposes

- paragraph 1 of schedule 8 “Statutory etc purposes” – the processing:
  (a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and
  (b) is necessary for reasons of substantial public interest.
- paragraph 2 of schedule 8 “Administration of justice” – the processing is necessary for the administration of justice.
- paragraph 6 of schedule 8 “Legal claims” – the processing:
  (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
  (b) is necessary for the purpose of obtaining legal advice, or
  (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
- paragraph 9 of schedule 8 “Archiving etc” – processing is necessary:
  (a) for archiving purposes in the public interest,
  (b) for scientific or historical research purposes, or
  (c) for statistical purposes.

In addition to the above grounds for sensitive processing, an Appropriate Policy that meets the requirements of section 42 of the DPA 2018 must be in place. This policy complies with the section 42 requirements.

6.4 Consent - The Office will request the consent of the data subject in writing in concise intelligible and easily accessible forms, using clear and plain language. To ensure the data subject is fully informed by the Office of the law enforcement purposes for which their personal data is being processed the information contained in the Office privacy notice will be provided separately. In circumstances where consent of the data subject is sought, the Office will ensure that:

- the consent is unambiguous
- the consent is given by affirmative action
- the consent is recorded as the condition for processing

7 Processing for the purposes of law enforcement

7.1 When conducting an investigation, the Office's primary purpose for processing personal data for law enforcement purposes is to comply with Part V11 the 1998 Act and all related regulations and legislation (see 5.1 above).

7.2 There may be circumstances when it will be necessary to process personal data for both law enforcement and non-law enforcement purposes. For example, there may be an investigation into several allegations of misconduct only some of which are potentially criminal. Personal data which the Office obtained for a law enforcement purpose may also be used in disciplinary investigations, proceedings and unsatisfactory performance proceedings. These purposes are authorised by the 1998 Act and associated regulations.

8 Processing personal data and sensitive processing for law enforcement purposes

8.1 In the course of our investigations, the Office will **process personal data and undertake** sensitive processing for law enforcement purposes from a number of different sources to include, but not limited to:

- an individual acting on behalf of a police force or any other data subject
- complainants
- Coroner's Service for Northern Ireland
- courts and tribunals
- family members
- forensic science officers and other experts
- government bodies and agencies
- health and social professionals
- legal representatives
- members of the public
- police and other law enforcement agencies
- Public Prosecution Service
- security agencies
- police officers and others subject of a complaint
- victims and survivors
- voluntary, charitable and non-governmental organisations
- witnesses

8.2 The Office may undertake sensitive processing data for law enforcement purposes from a range of categories of data subjects in the course of its investigations. These include, but are not limited to:

- complainants
- members of the public
- police officers and others subject to a complaint
- victims and survivors
- witnesses

8.3 The Office will disclose personal data only in accordance with the provisions of Part 3 of DPA 2018. In relation to sensitive processing it will only disclose that data with third parties where *strictly necessary* for the purposes of its statutory functions and in compliance with Section 63 of the 1998 Act (please see Appendix A for full text and the Office's Privacy Notice at www.policeombudsman.org)

8.4 Criminal offence data is routinely processed in the course of the assessment, investigation and reporting on complaints. However the Office does not keep a register of criminal convictions. Neither is that data disclosed except where permitted pursuant to section 63 of the 1998 Act.

9 Ensuring Compliance with the Data Protection Principles

9.1 Part 3 of the DPA 2018 provides for the data protection principles for processing personal data and for undertaking sensitive processing for law enforcement purposes. The Office ensures compliance as follows:

Accountability principle:

9.2 The Office has put in place appropriate technical and organisation measures to meet the requirements of accountability. These include:

- The appointment of a Data Protection Officer who reports directly to the CEO and Ombudsman.
- Integrating the concept of 'data protection by design and default' into all processes and activities.
- Maintaining adequate records of its processing activities.
- Adopting and implementing data protection policies and ensuring the Office has appropriate data sharing agreements in place that are compliant with the DPA 1998.
- Ensuring regular monitoring and maintenance of policies concerning data protection issues.
- Implementing appropriate security measures in relation to the personal data processed.
- Carrying out data protection impact assessments for high risk processing.

9.3 The Office will regularly review its accountability measures and update or amend them when required.

Section 35 - the first data protection principle: Lawful and fair

9.4 Processing for law enforcement purposes must be lawful and fair. It is only lawful to the extent it is based on law and either the data subject has given their consent for the processing or the processing is necessary for the law enforcement purpose or the processing meets one of the conditions in schedule 8. The Office acts lawfully and in compliance with the 1998 Act and related legislation and regulations (see Appendix B).

9.5 Our processing for law enforcement purposes satisfies the first schedule 8 condition that it is necessary for the exercise of a function conferred on the Police Ombudsman for the purposes of the legislation listed in Appendix B. The conditions for sensitive processing for law enforcement purposes are satisfied as outlined at 5.1 above.

9.6 The Office uses Privacy Notices to inform data subjects of the purpose for which their personal data is processed and these can be found at www.policeombudsman.org

Section 36 - the second data protection principle: Specified, explicit and legitimate and processed for the purpose it was collected

9.7 The Office processes personal data for the law enforcement purposes listed at section 31 of the DPA 2018. Law enforcement defined at 2.5 of this policy. When processing personal data for law enforcement purposes or undertaking sensitive processing, the Office specifies the purpose for which the data is processed and is explicit about the manner in which the data is processed and any intended disclosure(s).

9.8 The Office collects personal data and undertakes sensitive processing solely for the purpose of its statutory functions for which it was collected and does not use that data for any incompatible purpose.

9.9 The Office may disclose the personal data obtained for any other law enforcement purposes provided this is authorised by law and the processing is necessary and proportionate to that other purpose. If the data is shared with another controller, we will document that they are authorized by law to process data for those purposes.

9.10 Personal data is collected and sensitive processing undertaken by the Office for the law enforcement purpose of investigating complaints of criminality and/or misconduct about police or the other bodies referred to in paragraph 4 above.

9.11 The Office maintains an Information Asset Register which details the purpose and legal basis for processing this data.

Section 37 - the third data protection principle: Adequate, relevant, not excessive as to what is necessary for the stated purposes

9.12 The Office does not systematically collect or harvest personal data for law enforcement purposes. The information that we process is necessary and proportionate for our purposes. When the Office processes personal data for any of the law enforcement purposes outlined at section 6 above, it ensures

that such processing is adequate, relevant and not excessive in relation to the purpose in which it was processed.

9.13 Where sensitive personal data is provided to us or obtained by us but is not relevant for the Office stated purposes, it will be erased. .

Section 38 - the fourth data protection principle: Accurate and, where necessary, kept up-to-date

9.14 The Office has put in place a Quality and Standards Board to ensure that a quality assurance framework exists and is being applied consistently in respect of key decision making concerning 'volume' complaints, complex current cases and historic cases. Personal information held in investigation files is checked for factual accuracy before onward disclosure to a third-party. Where the Office becomes aware that personal data or sensitive processing for law enforcement purposes is inaccurate, having regard to the purpose for which it is being processed, it will take every reasonable step to ensure whenever possible that this is erased or rectified without delay. The reasons for the decision not to rectify or seek rectification will be documented.

9.15 The Office will take reasonable steps to ensure that inaccurate or incomplete personal data will not be transmitted or disclosed for any of the law enforcement purposes, Steps will be taken to verify data before sending it externally or publishing it .The recipient will be provided the necessary information to verify and assess the accuracy of the data we hold. If after onward transmission, the Office is aware that personal data was in correct and should not have been transmitted, the recipient will be informed as soon as possible. All decisions made to make personal data available will be documented.

9.16 There are procedures incorporated into the Office's investigation of complaints to ensure good data quality. Staff are aware of their obligations to update complainant personal details as soon as notified of a change. In doing so, staff are conscious this can affect a number of cases and therefore data changes cascade through the case management system. The Office regularly receives an updated copy of the Nominal Roll from PSNI which provides the most current details of all police officers within the PSNI and is directly uploaded to the Case Handling System (CHS). Template documents attached to the CHS can be amended and updated as appropriate on a system wide basis to ensure the information held is current.

9.17 The Office will, where relevant, and as far as possible, distinguish between personal data relating to different categories of data subject, such as people suspected of committing an offence, or people convicted of committing and offence, suspects or victims of a criminal offence and witnesses or other people who have information about police criminality or misconduct. This processing will only be undertaken where the data is relevant to the purpose being pursued.

9.18 The Office does not undertake automated decision making in relation to personal data or sensitive processing for law enforcement purposes..

Section 39 - the fifth data protection principle: Retained for no longer than necessary

9.19 The Office has a Disposal and Retention schedule which lists the data held and how long it is held for and it available here(link). The schedule is maintained under active consideration, based on advice from the Public Records Office NI (PRONI) and regularly reviewed by the Office and approved by the NI Assembly. We have a Memorandum of Understanding with PRONI to help ensure compliance. For example, prior to transfer to PRONI, an investigative file is reviewed by the investigating officer and subsequently by a senior investigating officer, to ensure that contents remain accurate and where necessary, up to date. This process includes agreement on the final disposition of the investigation and the appropriate timescales in accordance with the Retention and Disposal Schedule.

Section 40 - the sixth data protection principle: Kept secure which includes protection against unauthorized or unlawful processing and against accidental loss, destruction or damage

9.20 Electronic information is processed within the Office's secure networks. Hard copy information is processed within secure premises. Electronic and hard copy processed for the law enforcement purposes is only available to staff who carry out the processing for these purposes. All electronic and physical storage have appropriate access controls applied.

9.21 The Office deploys a wide range of technical and procedural controls (outlined at Appendix C) in order to protect personal data and sensitive processing for law enforcement purposes. These controls are under the oversight of the Information Assurance Security Group, (IASG). IASG's principal aim is to oversee all functional data protection and ensure all directorates comply with relevant information security standards. Residual information risk is accepted on behalf of the Office by the Senior Information Risk Owner (the Chief Executive).

9.22 The Office reviews and revises tall data protection policies and controls as appropriate to ensure the highest standards of data security as part of ongoing information assurance checks.

Section 41 – Safeguards: archiving

9.23 The Office undertakes sensitive processing for law enforcement purposes where the processing is necessary for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes. The processing is not permitted if it is carried out for the purposes of, or in connection with, measures or decisions with respect to a particular data subject, or it is likely to cause substantial damage or substantial distress to a data subject.

9.24 The Office will transfer any information identified by the Public Records Office NI which falls within their remit, as per the Retention and Disposal Schedule.

Section 42 – Safeguards: sensitive processing

9.25 The Office is required to have an 'Appropriate Policy' when undertaking sensitive processing for law enforcement purposes. This policy satisfies the

requirements of section 42 and is therefore an Appropriate policy document in support of the office compliance with the first data protection principle at section 35 (5) of the DPA 2018. A copy of this policy will be made available to the Information Commissioner on request and without charge.

10 Other related policies

10.1 This policy should be read in conjunction with all other relevant policies and materials issued by the office and available on its website.

11 Retention and Review of this Policy Document

11.1 This policy will be retained for the duration of our processing and for a minimum of 6 months after processing ceases.

11.2 This policy will be reviewed every three years or revised more frequently if necessary.

APPENDIX A: Section 63 of the Police (Northern Ireland) Act 1998

Restriction on disclosure of information.

63. –
(1) No information received by a person to whom this subsection applies in connection with any of the functions of the Ombudsman under this Part shall be disclosed by any person who is or has been a person to whom this subsection applies except-

- (a) to a person to whom this subsection applies;
- (b) to the Department of Justice or the Secretary of State;
- (c) to other persons in or in connection with the exercise of any function of the Ombudsman;
- (ca) for the purposes of an inspection of the Ombudsman carried out by the Chief Inspector of Criminal Justice in Northern Ireland under Part 3 of the Justice (Northern Ireland) Act 2002; [added SR (NI) 2002/414 from 20 Dec 2002]
- (d) for the purposes of any criminal, civil or disciplinary proceedings; or
- (e) in the form of a summary or other general statement made by the Ombudsman which-
  - (i) does not identify the person from whom the information was received; and
  - (ii) does not, except to such extent as the Ombudsman thinks necessary in the public interest, identify any person to whom the information relates.

(2) Subsection (1) applies to-

- (a) the Ombudsman; and
- (b) an officer of the Ombudsman.

(2A) [added from 4 Nov 2001, am. 2003 c.6 from 8 April 2003] Subsection (1) does not prevent the Ombudsman, to such extent as he thinks it necessary to do so in the public interest, from disclosing in a report of an investigation under section 60A-

- (a) the identity of an individual, or
- (b) information from which the identity of an individual may be established.

(3) Any person who discloses information in contravention of this section shall be guilty of an offence and liable on summary conviction to a fine not exceeding level 5 on the standard scale.

(4) Nothing in subsection (1)(b) permits the disclosure to the Department of Justice of information—

- (a) which has been supplied to the Ombudsman under section 66(1) of the Police (Northern Ireland) Act 2000(a) for the purposes of or in connection with an investigation under section 60A of this Act, and
- (b) in relation to which the Ombudsman has been informed under section 66(3)(b) of the Police (Northern Ireland) Act 2000 that the information is, in the opinion of the Chief Constable or the Board, information which ought not to be disclosed on the ground mentioned in section 76A(1)(a) of that Act.

APPENDIX B: Relevant Legislation and Regulations

The legislation which governs the work of the Police Ombudsman's Office is Part VII of the Police (Northern Ireland) Act 1998.

The following is a list of some of the legislation and regulations which also regulates the work of the Office:

Legislation

- Anti-terrorism, Crime and Security Act 2001
- Criminal Appeal Act 1995
- Criminal Justice and Police Act 2001
- Criminal Law Act (NI) 1967
- Criminal Procedure and Investigations Act 1996
- Data Protection Act 2018
- Freedom of Information Act 2000
- Human Rights Act 1998
- Investigatory Powers Act 2016
- Justice (Northern Ireland) Act 2000
- Justice (Northern Ireland) Act 2002
- Justice (Northern Ireland) Act 2004
- Northern Ireland Act 1998
- Police (Northern Ireland) Act 1998
- Police (Northern Ireland) Act 2000
- Police (Northern Ireland) Act 2003
- Proceeds of Crime Act 2002
- Regulation of Investigatory Powers Act 2000
- The Police and Criminal Evidence (application to the Police Ombudsman) Order (NI) 2009
- The Serious Organised Crime and Policing Act 2005

Orders in Council

- The Commissioner for Children and Young People (Northern Ireland) Order 2003
- The Police (Northern Ireland) Act 1998 (Modification) Order 2003
- Criminal Justice (Northern Ireland) Order 2004
- Criminal Justice (Northern Ireland) Order 2005

- The Policing (Miscellaneous Provisions) (Northern Ireland) Order 2007

Statutory Rules

- Statutory Rule 1989 No. 1341: The Police and Criminal Evidence Order (Northern Ireland) 1989
- Statutory Rule 2000 No. 314: The Police and Criminal Evidence (Application to Police Ombudsman) Order (Northern Ireland) 2000
- Statutory Rule 2000 No. 315: The Royal Ulster Constabulary (Conduct) Regulations 2000
- Statutory Rule 2000 No. 316: The Royal Ulster Constabulary (Unsatisfactory Performance) Regulations 2000
- Statutory Rule 2000 No. 317: The Royal Ulster Constabulary (Appeals) Regulations 2000
- Statutory Rule 2000 No. 318: The Royal Ulster Constabulary (Complaints etc.) Regulations 2000
- Statutory Rule 2000 No. 319: The Royal Ulster Constabulary (Complaints) (Informal Resolution) Regulations 2000
- Statutory Rule 2000 No. 320: The Royal Ulster Constabulary (Conduct) (Senior Officer) Regulations 2000
- Statutory Rule 2000 No. 399: The Police (Northern Ireland) Act 1998 (Commencement) Order (Northern Ireland) 2000
- Statutory Rule 2000 No 412: The Police (Northern Ireland) Act 2000 (Commencement) Order 2000
- Statutory Rule 2001 No.132: The Police (Northern Ireland) Act 2000 (Commencement No. 2) Order 2001
- Statutory Rule 2001 No. 184: Royal Ulster Constabulary (Complaints etc) Regulations 2001
- Statutory Rule 2001 No. 396: The Police (Northern Ireland) Act 2000 (Commencement No.3 and Transitional Provisions) Order 2001
- Statutory Rule 2001 No. 369: Police Trainee Regulations (NI) 2001
- Statutory Rule 2003 No.184: Police Service of Northern Ireland (Amendment) Regulations 2003
- Statutory Rule 2003 No. 68: Police Service of Northern Ireland (Conduct) Regulations 2003
- Statutory Rule 2003 No.142: Police (Northern Ireland) Act 1998 (Commencement No.5) Order (Northern Ireland) 2003
- Statutory Rule 2003 No. 399: Police Service of Northern Ireland (Appeals) (Amendment) Regulations 2003
- Statutory Rule 2004 No.122: The Police Service of Northern Ireland (Secondment) (Garda Síochána) Regulations 2004
- Statutory Rule No. 376: The Police (Northern Ireland) Act (Modification) Order 2003

- Statutory Rule 2004 No. 315: Police Service of Northern Ireland (Conduct etc.) (Amendment) Regulations 2004
- Statutory Rule 2004 No. 379: Police (Appointments) Regulations (Northern Ireland) 2004
- Statutory Rule 2005 No. 341: The Police Service of Northern Ireland (Complaints etc.) (Amendment) Regulations 2005
- Statutory Rule 2006 No. 69: The Police (Recruitment) (Amendment) Regulations (Northern Ireland) 2006
- Statutory Rule 2007 No.177: The Police (Northern Ireland) Act 2003 (Commencement No.2) Order 2007
- Statutory Rule 2007 No.58: Police and Criminal Evidence (Northern Ireland) Order 1989 (Code of Practice) (No.3) Order 2007
- The Police and Criminal Evidence (Amendment) (Northern Ireland) Order 2007
- Statutory Rule 2007 No.130: Police Service of Northern Ireland (Unsatisfactory Performance and Attendance) Regulations 2007
- Police Powers for Designated Staff (Complaints and Misconduct) Regulations (NI) 2008

Statutory Instruments

- The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003
- The Regulation of Investigatory Powers (Communications Data) Order 2003
- The Criminal Justice (No 2) (Northern Ireland) Order 2004
- Policing (Miscellaneous) Provisions (Northern Ireland) Order 2007
- Northern Ireland Act 1998 (Devolution of Policing and Justice) Order 2010

APPENDIX C: Controls for the Security of Personal Data

Controls include but are not limited to:

- Memorandums of Understanding with other law enforcement agencies in compliance with ICO data sharing guidance and Codes of Practice
- Induction and mandatory annual Information Security Training for all staff
- Acceptable use of IT equipment and systems defined in Security Operating Procedures signed by all users of the Office's systems
- Role Based Access Controls, limiting the Office's system users to only access those systems necessary for them to perform their duties
- Identity and access management through Human Resources hiring and reference polices, including HMG Security Clearances.
- Appropriate prevention of the Office's core IT system (e.g. firewalls, malware detection and defence)
- Encryption of data in transit across dedicated Office networks where appropriate
- Monitoring and/or logging of digital and user activity into, within and out of the Office's systems
- Independent accreditation of the Office systems
- Annual and ad-hoc IT health checks and penetration tests by independent certified test teams; with follow-up treatment of identified vulnerabilities
- Clear desk policy in all departments and at all levels
- Robust procedures for the reporting of any data or potential data breaches.